Ukraine's IT army is a world first: Here's why it is an important part of the war

October 25 2023, by Vasileios Karagiannopoulos

Credit: Unsplash/CC0 Public Domain

Ukraine's recently formed "IT army" is playing a crucial role in the war with Russia, launching disruptive cyber-attacks and data thefts against the Russian government and other high-profile targets such as energy

giant Gazprom.

The IT army has thousands of volunteer members around the world, who use Twitter and Telegram channels to communicate, coordinate and report on actions. Its members have already taken part in a wide variety of attacks. These range from stealing and exposing important information to successfully disrupting Russian communications and other critical networks in order to hinder the Russian war efforts.

The formation of the IT army was a Ukrainian government response to concerns about the role Russian cyber-attacks might have on the war. On February 26 2022 Ukrainian vice-prime minister Mykhailo Fedorov issued a call to arms to all hackers willing to join its IT army and support Ukraine against Russian cyber-attacks and to disrupt Russian networks.

The creation of Ukraine's IT army is considered a world first in cyber-warfare operations. It is believed to be the first time a state official has openly called on hackers from around the globe to join a nation's military defensive efforts against an invading force and act as part of its hybrid military operations.

Ukraine's IT army are also supported by hacktivist groups which are not affiliated with Ukraine, but want to support the country against Russia.

One of its most disruptive attacks was carried out in 2022 and targeted Russia's authentication system, Chestny Znak, which adds a unique ID and barcode to all products in the country.

This cyber-attack flooded Chestny Znak's servers with information, causing it to stop working, creating widespread disruption with serious economic costs and even leading the Russian government to abolish certain labeling policies.

The IT army and other hacktivist groups have also managed to target Russian radio and TV stations to add snippets of videos about the war in Ukraine to programs and to broadcast fake air raid alerts. For example, in June 2023, Russian state TV and other channels were hacked and broadcast a video allegedly created by the Ukrainian ministry of defense including footage of Ukraine's military operations, followed by a message reading "the hour of reckoning has come" in Ukrainian.

This rallying of hackers for Ukraine has prompted a response from groups within Russia, such as Killnet, Sandworm and XaKnet, to launch their own cyber-attacks on Ukrainian and western targets. However, Russian cyber-attacks started well before the invasion and intensified in February 2022. These involved an array of smaller assaults on Ukrainian state and private networks and even a major cyber-attack on the Viasat satellite communications system in order to prevent the monitoring of Russian troop movements during the invasion.

International ramifications

The Viasat cyber-attack on February 23 had serious spillover effects outside Ukraine's borders, affecting thousands of German wind turbines by shutting down their remote control systems. This incident showed that all wars now have a very real cyberspace dimension that could have global implications outside the war zone.

Apart from the global cybersecurity concerns that this conflict has generated, the creation of the IT army has sparked important discussions around the role of cyberwarfare in real-life military operations. One significant question is whether groups such as the IT army could be considered combatants, rather than civilians, which can impact whether they can be legally targeted by Russian military, losing some of the protections afforded by international law.

Having said that, some countries, including Estonia, already have formally established similar cyberforce reserves. This is something that is currently under consideration by the Ukrainian government for its IT army.

Another consideration is the unpredictability of hacker groups operating as decentralized "cyberguerillas". This could have serious spillover effects beyond the war zone, potentially resulting in escalation across more countries.

Efforts have been made by the international community and academic experts to apply the law of war and international humanitarian law to cyberoperations, which have culminated in the publication of the Tallinn manuals. These manuals attempt to cover issues of international law regarding cyber incidents. But many of the concerns that the IT army has brought to the fore remain contested, especially since these documents are not binding.

Conflicts could become even more complex as AI tools are increasingly used in cyber-attacks and gradually become part of modern information warfare in the next few years.

This is why we need more concerted efforts to resolve the practical and legal concerns, before the new age of cyberwarfare is upon us.

Provided by The Conversation

world-important-war.html